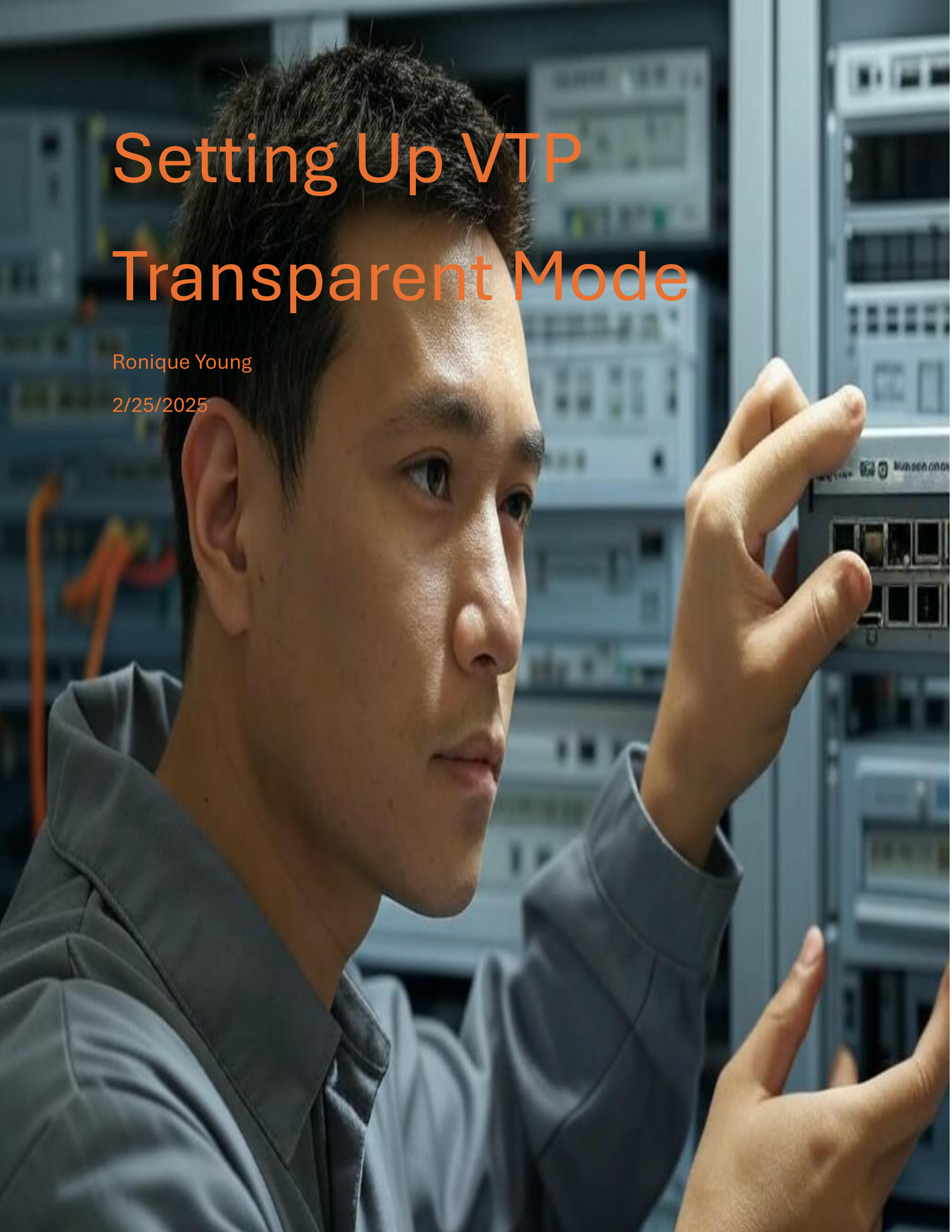


Setting Up VTP Transparent Mode

Ronique Young

2/25/2025

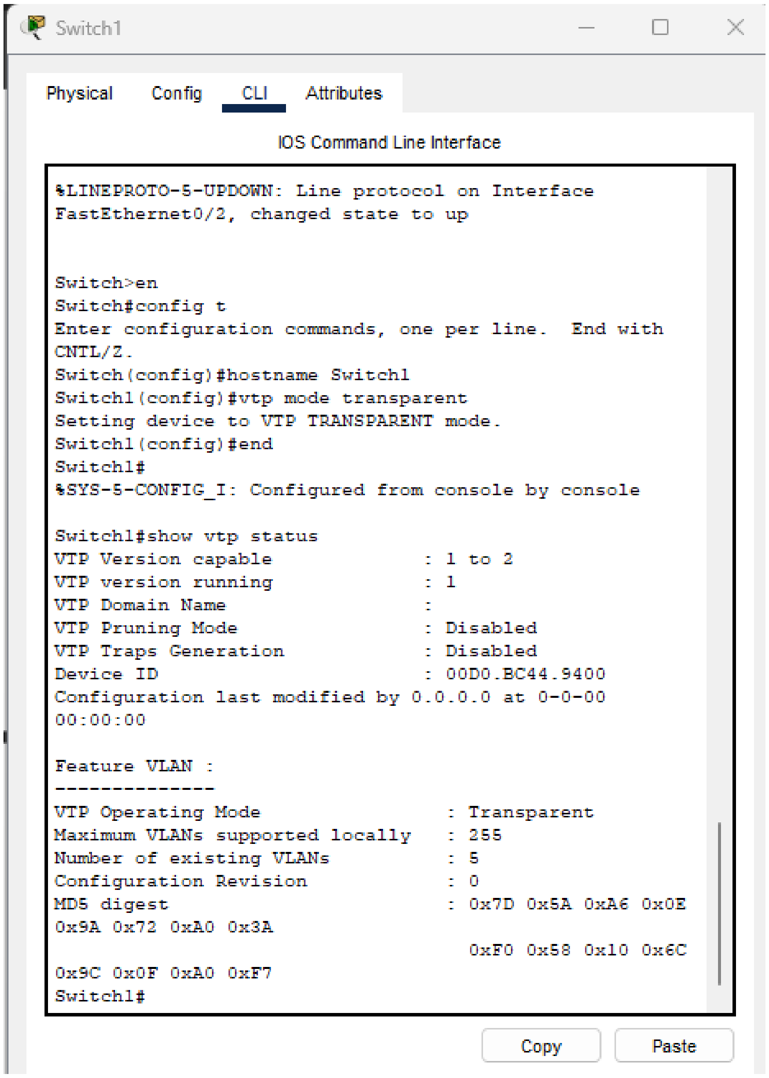
Project Showcase: Configuring VTP Transparent Mode on Cisco Catalyst Switches

Lab Objective:

In this project, I aimed to master the configuration of VTP Transparent mode on Cisco Catalyst Switches, demonstrating a deep understanding of VLAN Trunking Protocol (VTP) operations. By default, Cisco switches operate as VTP servers, but I focused on reconfiguring them to operate in Transparent mode—a critical skill for managing VLANs in enterprise network environments.

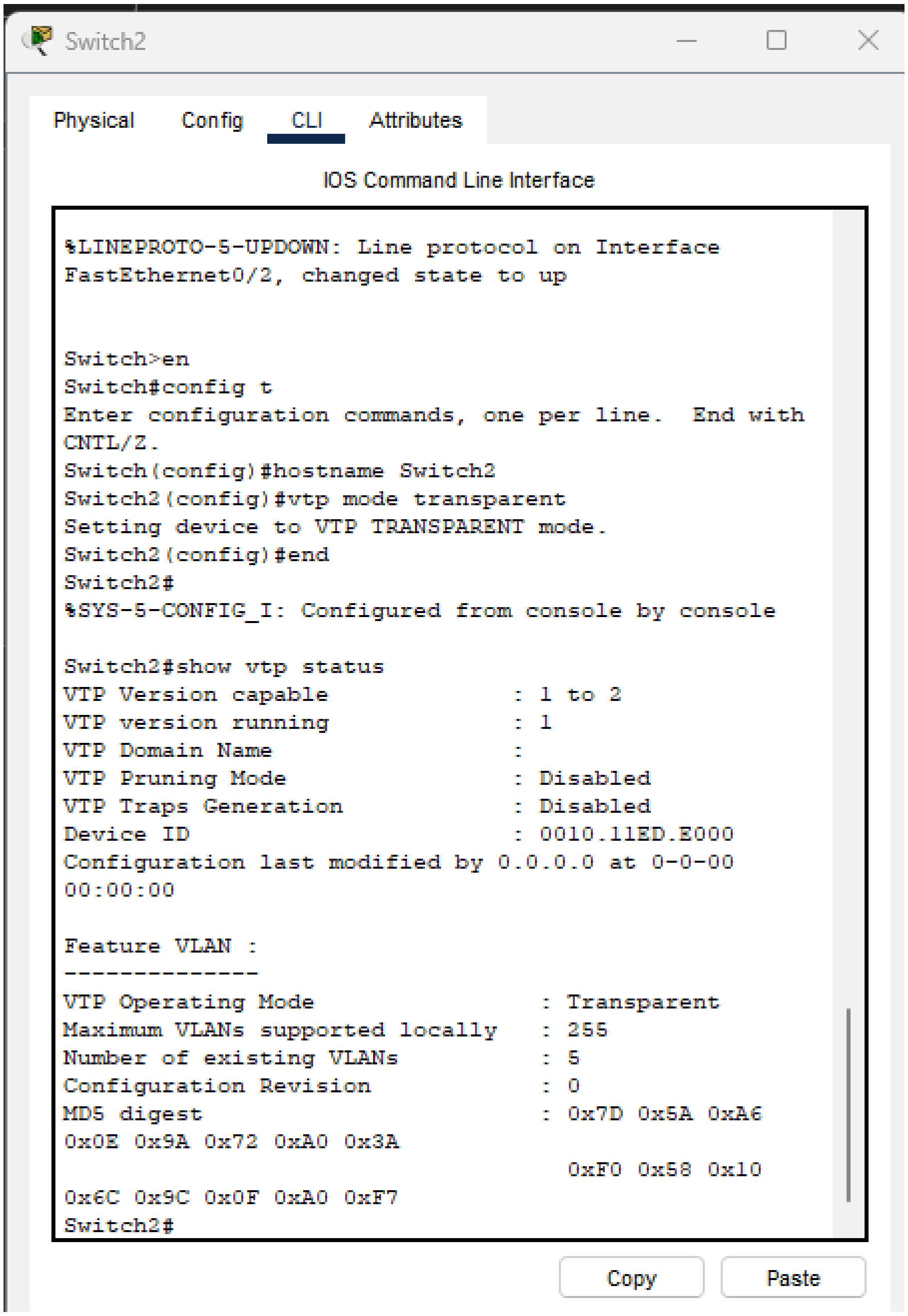
Lab Purpose & Impact:

Configuring VTP Transparent mode is an essential competency that I've developed through this hands-on lab. Unlike VTP server mode, where VLAN configurations automatically propagate across switches in the same VTP domain, Transparent mode requires manual VLAN setup, offering greater control over network segmentation. My work ensured that VLANs configured on the switch remained local and were not shared, while still enabling seamless traffic forwarding to other switches via trunk links. This project showcases my ability to implement precise, secure, and efficient network designs tailored to specific operational needs.



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to up


Switch>en
Switch#config t
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#hostname Switch1
Switch1(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch1(config)#end
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 00D0.BC44.9400
Configuration last modified by 0.0.0.0 at 0-0-00
00:00:00

Feature VLAN :
--------------
VTP Operating Mode                : Transparent
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x7D 0x5A 0xA6 0x0E
0x9A 0x72 0xA0 0x3A
                                    0xF0 0x58 0x10 0x6C
0x9C 0x0F 0xA0 0xF7
Switch1#
```

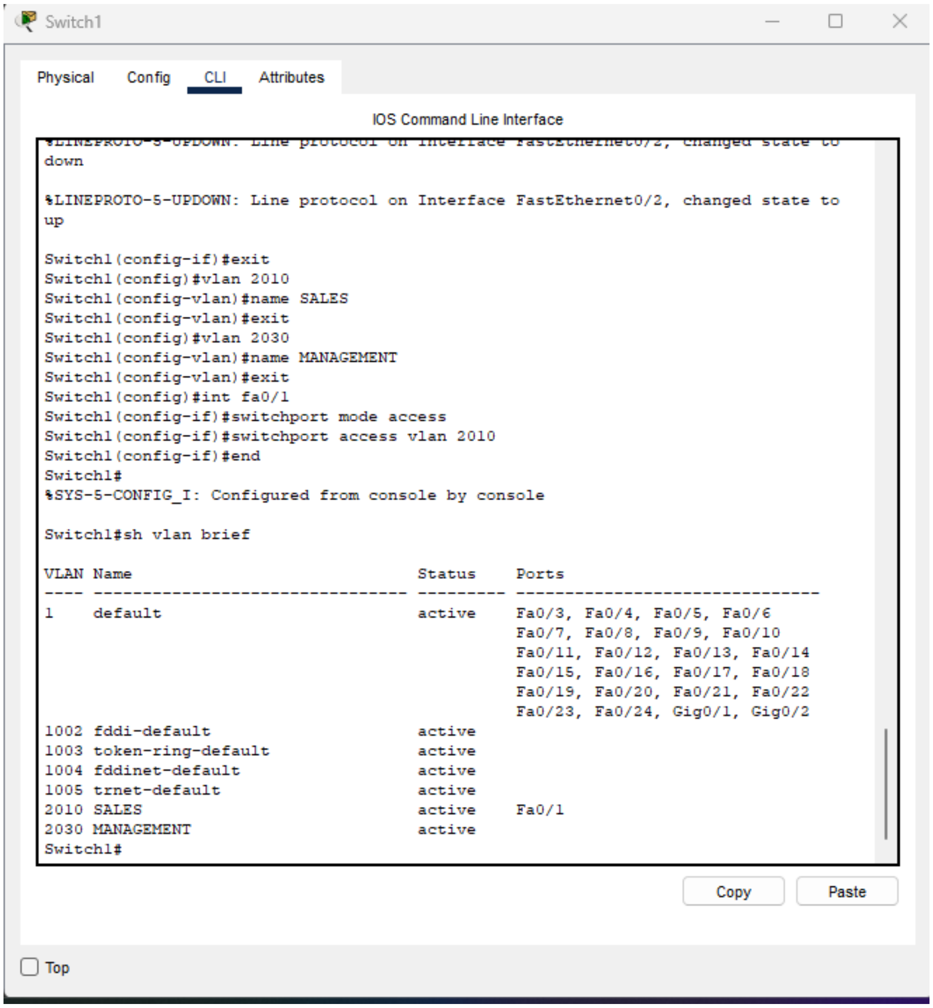
For this project, I started by setting up the foundational network configurations to ensure everything would run smoothly for the VLAN setup. My first step was to configure hostnames on a couple of switches—Switch 1 and Switch 2—and two routers, Router 1 and Router 3, following the layout provided in the network topology. This helps keep everything organized and easy to identify as the network grows.



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to up


Switch>en
Switch#config t
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#hostname Switch2
Switch2(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch2(config)#end
Switch2#
%SYS-5-CONFIG_I: Configured from console by console

Switch2#show vtp status
VTP Version capable                : 1 to 2
VTP version running                : 1
VTP Domain Name                    :
VTP Pruning Mode                   : Disabled
VTP Traps Generation               : Disabled
Device ID                          : 0010.11ED.E000
Configuration last modified by 0.0.0.0 at 0-0-00
00:00:00

Feature VLAN :
--------------
VTP Operating Mode                   : Transparent
Maximum VLANs supported locally      : 255
Number of existing VLANs             : 5
Configuration Revision               : 0
MD5 digest                           : 0x7D 0x5A 0xA6
0x0E 0x9A 0x72 0xA0 0x3A
                                       0xF0 0x58 0x10

0x6C 0x9C 0x0F 0xA0 0xF7
Switch2#
```

Next, I focused on getting the switches ready for VLANs by configuring and verifying that both Switch 1, and Switch 2 were operating in VTP Transparent mode. I chose this mode because it gives us more control over VLAN updates, preventing automatic changes from propagating unexpectedly. I also set both switches to be part of the same VTP domain, which I named 'CISCO.' This step is crucial because, for VLAN information to be shared between switches over a trunk link, they need to be in the same VTP domain. Once that was in place, I verified everything was working as expected, ensuring a solid base for the rest of the VLAN configuration.

Task 3:

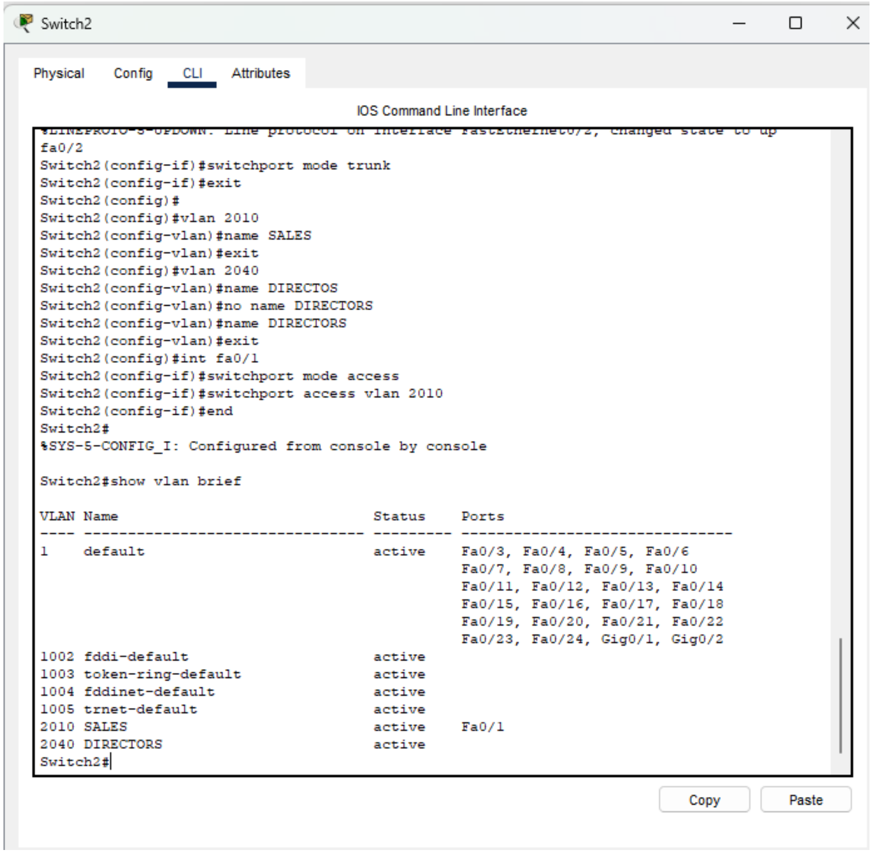


```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to
up

Switch1(config-if)#exit
Switch1(config)#vlan 2010
Switch1(config-vlan)#name SALES
Switch1(config-vlan)#exit
Switch1(config)#vlan 2030
Switch1(config-vlan)#name MANAGEMENT
Switch1(config-vlan)#exit
Switch1(config)#int fa0/1
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 2010
Switch1(config-if)#end
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
2010 SALES                            active    Fa0/1
2030 MANAGEMENT                       active
Switch1#
```

To address Task 3, I started by configuring the trunk link between Switch 1 and Switch 2, which is a foundational step for enabling VLAN communication across the switches. Specifically, I set the FastEthernet0/1 interface on both switches as an 802.1Q trunk. This encapsulation method is essential because it tags VLAN traffic, allowing the switches to share VLAN information effectively. I opted for 802.1Q due to its widespread support and compatibility with various devices. Once configured, I verified that the trunk was operational, ensuring the link was active and ready to carry VLAN traffic.

Next, I moved on to configuring the VLANs on Switch 1. I created VLAN 2010 and VLAN 2030, assigning each the specific names outlined in the project guidelines. Naming VLANs is a critical practice, particularly in larger networks, as it enhances clarity and helps administrators quickly understand each VLAN’s purpose. After setting up the VLANs, I confirmed their configurations to ensure the IDs and names were correct. Then, I configured the

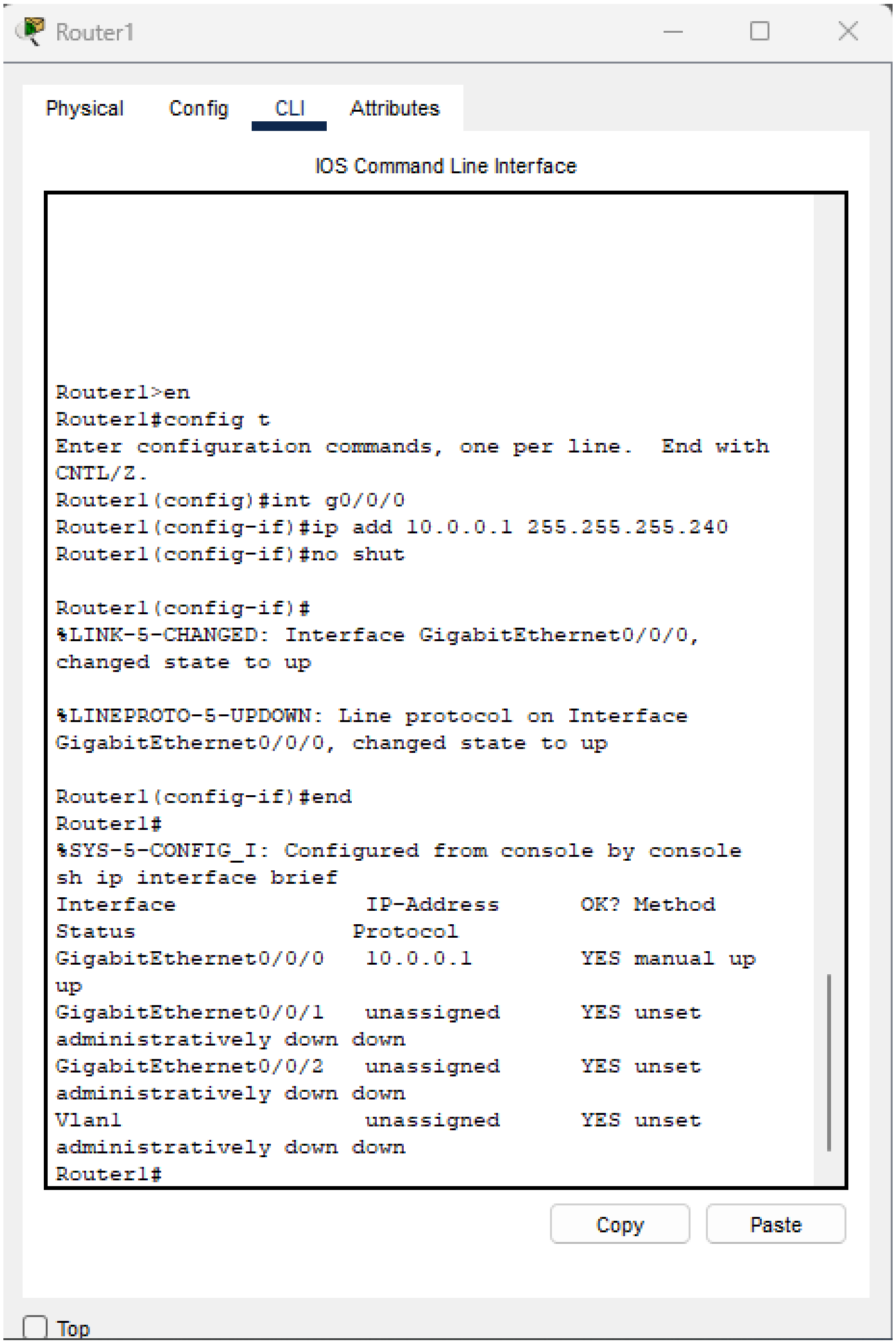
FastEthernet0/1 interface on Switch 1 as an access port and assigned it to VLAN 2010. This setup ensures that any device connected to this port becomes part of VLAN 2010. I double-checked the port assignment to verify it was active and properly linked to the VLAN.



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
fa0/2
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#exit
Switch2(config)#
Switch2(config)#vlan 2010
Switch2(config-vlan)#name SALES
Switch2(config-vlan)#exit
Switch2(config)#vlan 2040
Switch2(config-vlan)#name DIRECTOS
Switch2(config-vlan)#no name DIRECTORS
Switch2(config-vlan)#name DIRECTORS
Switch2(config-vlan)#exit
Switch2(config)#int fa0/1
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 2010
Switch2(config-if)#end
Switch2#
%SYS-5-CONFIG_I: Configured from console by console

Switch2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
2010 SALES                            active    Fa0/1
2040 DIRECTORS                        active    
Switch2#
```

Following that, I shifted focus to Switch 2, where I configured VLAN 2010 and VLAN 2040, again adhering to the specified naming conventions. Maintaining consistent naming across switches is vital for a cohesive network structure. After creating and verifying these VLANs, I set the FastEthernet0/1 interface on Switch 2 as an access port and assigned it to VLAN 2010, mirroring the configuration on Switch 1. This allows devices connected to this port to join VLAN 2010 and communicate with devices on Switch 1 via the trunk link. I verified the port configuration to confirm it was correctly assigned and functioning.

Finally, I conducted a thorough verification of the entire setup to ensure everything was working as intended. I rechecked the trunk link to confirm it was successfully carrying VLAN traffic. I also reviewed the VLAN configurations on both switches, verifying that VLAN 2010, VLAN 2030 on Switch 1, and VLAN 2040 on Switch 2 were all properly established with the correct names. Additionally, I confirmed that the access ports on both switches were accurately assigned to VLAN 2010. This comprehensive verification process guarantees proper network segmentation, enabling devices in VLAN 2010 to communicate across the switches while keeping VLAN 2030 and VLAN 2040 ready for their designated purposes.



```
Router1>en
Router1#config t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router1(config)#int g0/0/0
Router1(config-if)#ip add 10.0.0.1 255.255.255.240
Router1(config-if)#no shut

Router1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to up

Router1(config-if)#end
Router1#
%SYS-5-CONFIG_I: Configured from console by console
sh ip interface brief
Interface              IP-Address      OK? Method
Status                Protocol
GigabitEthernet0/0/0   10.0.0.1        YES manual up
up
GigabitEthernet0/0/1   unassigned      YES unset
administratively down down
GigabitEthernet0/0/2   unassigned      YES unset
administratively down down
Vlan1                  unassigned      YES unset
administratively down down
Router1#
```

For Task 5, I began by setting up the IP addressing on the routers to establish connectivity within the network. Specifically, I configured the Gigabit Ethernet interface on Router 1 (R1) with the IP address 10.0.0.1 and a subnet mask of /28. This subnet mask provides a small, efficient address space suitable for the network's needs. Then, I moved to Router 3 (R3) and configured its Gigabit Ethernet interface with the IP address 10.0.0.3, using the same /28 subnet mask to ensure both routers were on the same subnet. Assigning these IP addresses correctly is crucial because it allows the routers to communicate with each other and serve as gateways for their respective segments of the network.

After configuring the interfaces, I tested the connectivity between VLANs by performing a ping test from R1 to R3. This step is a practical way to verify that the network is functioning as expected, ensuring that packets can travel between the routers. I initiated the ping from R1 targeting 10.0.0.3, R3's IP address, and monitored the response. A successful ping would indicate that the interfaces were properly configured, the link between the routers was active, and the VLAN setup was allowing traffic to flow as intended. If the ping failed, I'd troubleshoot by checking the interface statuses, IP configurations, and any potential issues with the VLAN or trunk configurations on the switches connecting these routers.

Once the ping succeeded, I confirmed that the configuration was solid. This process not only validated the IP setups on R1 and R3 but also ensured that the broader network—including the VLANs and trunk links—was working cohesively. By assigning these specific IP addresses and testing connectivity, I established a reliable communication path between the routers, which is essential for supporting any additional network services or traffic that would rely on this setup.